

10-02-00

A

Please type a plus sign (+) inside this box



Approved for use through 09/30/2000 OMB 0651-0032  
 Patent and Trademark Office U.S. DEPARTMENT OF COMMERCE  
 Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

# UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 042390.P1144  
 First Inventor or Application Identifier Robert P. Hale  
 Title A SYSTEM AND METHOD FOR VERIFYING THE INTEGRITY OF  
 Express Mail Label No. EL466331508US

## APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

## ADDRESS TO:

Assistant Commissioner for Patents  
 Box Patent Application  
 Washington, DC 20231

1. ☒ Free Transmittal Form  
 (Submit an original, and a duplicate for fee processing)

2. ☒ Specification [Total Pages 20]  
 (preferred arrangement set forth below)

- Descriptive title of the invention  
 - Cross References to Related Applications  
 - Statement Regarding Fed sponsored R & D  
 - Reference to Microfiche Appendix  
 - Background of the Invention  
 - Brief Summary of the Invention  
 - Brief Description of the Drawings (if filed)  
 - Detailed Description  
 - Claim(s)  
 - Abstract of the Disclosure

3. ☒ Drawing(s) (35 U.S.C. 113) [Total Sheets 2]

Oath or Declaration [Total Pages 4]

- a. ☐ Newly executed (original copy)  
 b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d))  
 (for continuation/divisional with Box 16 completed)  
 i. ☐ **DELETION OF INVENTOR(S)**  
 Signed statement attached deleting  
 inventor(s) named in the prior application,  
 see 37 CFR §§ 1.63(d)(2) and 1.33(b).

\*NOTE FOR ITEMS 1 & 3: IN ORDER TO BE ENTITLED TO PAY SMALL  
 ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R.  
 § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED  
 UPON (37 C.F.R. § 1.28).

5. ☐ Microfiche Computer Program (Appendix)

6. Nucleotide and/or Amino Acid Sequence Submission  
 (if applicable, all necessary)

- a. ☐ Computer Readable Copy  
 b. ☐ Paper Copy (identical to computer copy)  
 c. ☐ Statement verifying identity of above copies

## ACCOMPANYING APPLICATION PARTS

7. ☐ Assignment Papers (cover sheet & document(s))  
 8. ☐ 37 C.F.R. § 3.73(b) Statement ☐ Power of Attorney  
 (when there is an assignee)  
 9. ☐ English Translation Document (if applicable)  
 10. ☐ Information Disclosure Statement (IDS)/PTO - 1449 ☐ Copies of IDS Citations  
 11. ☐ Preliminary Amendment  
 12. ☐ Return Receipt Postcard (MPEP 503)  
 (Should be specifically itemized)  
 13. ☐ \*Small Entity ☐ Statement filed in prior application,  
 Statement(s) Status still proper and desired  
 14. ☐ Certified Copy of Priority Document(s)  
 (if foreign priority is claimed)  
 15. ☐ Other:

16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No:

Prior application Information: Examiner

Group/Art Unit

For CONTINUATION or DIVISIONAL APPS only. The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

## 17. CORRESPONDENCE ADDRESS

☐ Customer Number of Bar Code Label

(insert Customer No. or Attach bar code label here)

or ☒ Correspondence address below

Name BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP  
 Address 12400 Wilshire Boulevard, Seventh Floor  
 City Los Angeles State California Zip Code 90025  
 Country U.S.A. Telephone (714) 557-3800 Fax (714) 557-3347

Name (Print/Type) William W. Schaal, Reg. No. 39,018

Signature

Date 09/29/00

Burden Hour Statement: This form is generated by EAS and hours to complete. Time will vary depending upon the needs of the individual case. Any comments or the amount of time you wish required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

09/29/00  
 09/29/00  
 09/29/00

Please type a plus sign (+) inside this box +

Approved for use through 09/30/2000 OMB 0651-0032  
Patent and Trademark Office U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

# FEE TRANSMITTAL for FY 2000

Patent fees are subject to annual revision.  
Small Entity payments must be supported by a small entity statement,  
otherwise large entity fees must be paid. See Forms PTO/SB/09-12,  
See 37 C.F.R. §§ 1.27 and 1.29.

TOTAL AMOUNT OF PAYMENT (\$) 1,314.00

Complete if known

Application Number  
Filing Date September 29, 2000  
First Named Inventor Robert P. Hale  
Examiner Name  
Group/Art Unit  
Attorney Docket No 042390.P9144

PTO/SB/17 (12/99)  
09/29/00  
09/29/00

## METHOD OF PAYMENT (check one)

1. ☒ The Commissioner is hereby authorized to charge indicated fees to  
☒ The Commissioner is hereby authorized to credit any over payments to

Deposit Account Number 02-2666  
Deposit Account Name Blakely, Sokoloff, Taylor & Zafman LLP

☒ Charge Any Additional Fees Required Under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20

2. ☒ Payment Enclosed:  
☒ Check ☐ Money Order ☐ Other

## FEE CALCULATION

### BASIC FILING FEE

Large Entity Fee Code	Fee (\$)	Small Entity Fee Code	Fee (\$)	Fee Description	Fee Paid
101	690	201	345	Utility filing fee	\$690.00
106	310	206	155	Design filing fee	
107	480	207	240	Plant filing fee	
108	690	208	345	Reissue filing fee	
114	150	214	75	Provisional filing fee	
SUBTOTAL (1)					\$ 690.00

### EXTRA CLAIM FEES

Large Entity Fee Code	Fee (\$)	Small Entity Fee Code	Fee (\$)	Fee Description	Fee Paid
33	20	13	18.00	Claims	\$234.00
8	3	5	78.00	Independent Claims	\$390.00
Multiple Dependent					

\*For number previously paid, if greater, For Reissues, see below

Large Entity Fee Code	Fee (\$)	Small Entity Fee Code	Fee (\$)	Fee Description	Fee Paid
103	18	203	9	Claims in excess of 20	
102	78	202	39	Independent claims in excess of 3	
104	260	204	130	Multiple Dependent claim, if not paid	
109	78	209	39	**Reissue independent claims over original patent	
110	18	210	9	**Reissue claims in excess of 20 and over original patent	
SUBTOTAL (2)					\$ 624.00

## FEE CALCULATION (continued)

### 3. ADDITIONAL FEE

Large Entity Fee Code	Fee (\$)	Small Entity Fee Code	Fee (\$)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet.	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	*Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	*Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for response within first month	
116	380	216	190	Extension for response within second month	
117	870	217	435	Extension for response within third month	
118	1,210	218	680	Extension for response within fourth month	
128	1,850	228	925	Extension for response within fifth month	
119	300	219	150	Notice of Appeal	
120	300	220	150	Filing a brief in support of an appeal	
121	260	221	130	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,210	241	605	Petition to revive - unintentional	
142	1,210	242	605	Utility issue fee (or reissue)	
143	430	243	215	Design issue fee	
144	580	244	290	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	790	246	395	Filing a submission after final rejection (37 CFR 1.129(a))	
149	790	249	395	For each additional invention to be examined (37 CFR 1.129(b))	
Other fee (specify)					
Other fee (specify)					

\* Reduced by Basic Filing Fee Paid

SUBTOTAL (3)

(\$)

## SUBMITTED BY

Typed or Printed Name William W. Schaal

Signature

Date

09/29/00

## Complete (if applicable)

Reg. Number 39,018

Deposit Account User ID 02-2666

Business Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231

UNITED STATES PATENT APPLICATION

FOR

**A SYSTEM AND METHOD FOR VERIFYING THE INTEGRITY OF  
STORED INFORMATION WITHIN AN ELECTRONIC DEVICE**

Inventor(s):

Robert P. Hale  
Andrew J. Fish

Prepared by:

Blakely, Sokoloff, Taylor & Zafman LLP  
12400 Wilshire Blvd., Suite 700  
Los Angeles, California 90025  
(714) 557-3800

## A SYSTEM AND METHOD FOR VERIFYING THE INTEGRITY OF STORED INFORMATION WITHIN AN ELECTRONIC DEVICE

### 1. Field

5       The present invention relates to the field of data security. More particularly, this invention relates to a scheme for verifying the integrity of stored information loaded within an electronic device.

### 2. General Background

10       Many electronic devices include a set of semi-permanently stored instructions referred to as firmware. For instance, computers include a type of firmware referred to as the basic input/output system (BIOS). Being executed by a processor of the computer, the BIOS is coded to perform various functions. For example, during a pre-boot cycle at power-up, the BIOS controls the initialization  
15 of the computer as well as the initialization of various hardware peripherals. Normally provided by a single vendor, the BIOS is loaded into pre-boot space of a non-volatile memory such as a read-only memory (ROM) component or a flash memory component during manufacture of the computer.

20       Recently, however, it has become desirable to store more sophisticated routines and data in the pre-boot space of the non-volatile memory. As an example, in recent efforts to protect against software viruses and malicious corruption of the BIOS, an image of the BIOS code may be digitally signed to produce a digital signature. Prior to execution of the BIOS, the digital signature may be used to determine whether the BIOS has been modified. This provides  
25 much needed virus protection.

Well known in the art, a digital signature is digital data signed using a private key of its signatory. Similar to encryption, the "signing process" may be accomplished using any of a number of software algorithms such as a Rivest Shamir and Adleman (RSA) algorithm or the Digital Signature Algorithm (DSA)  
30 as set forth in a Federal Information Processing Standards publication 186 entitled "Digital Signature Standard" (May 19, 1994). Normally, the digital data is placed  
042390.P9144

in an encoded form (referred to as the “hash value”), achieved by performing a one-way hash operation on the original digital data, prior to signing the hash value. The term “one-way” indicates that there does not readily exist an inverse operation or function to recover any discernible portion of the digital data from the hash value.

Recently, the computer industry has made efforts to develop BIOS as a collection of software modules produced by different vendors rather than a piece of monolithic code produced by a single vendor. It is likely that the code of the BIOS modules would be configured as “execute-in-place” modules because this code would be executed before the availability of system random access memory (RAM). Also, it is likely that relocation would be used to properly load the BIOS modules within the non-volatile memory because it would be too difficult for all of the BIOS vendors to agree on the specific addressing scheme beforehand.

As commonly known in the industry, “relocation” is a process by which addresses within each BIOS module are adjusted based on the particular address location in memory allotted for the BIOS module (referred to as the “base address”). Thus, software routines within a BIOS module are usually coded with relative offsets from a base address that has not yet been assigned. During relocation, the addresses of various software routines within the BIOS module would be adjusted by adding the base address to each of the relative offsets.

Unfortunately, if relocation is performed on the execute-in-place BIOS modules, any digital signatures associated with the images of the BIOS modules would be ineffective because any data integrity analysis using the digital signatures would indicate that the BIOS module has been modified. Hence, it is virtually impossible to determine whether modification of the BIOS module was unauthorized or merely due to the relocation operation. Thus, it would be desirable to develop an integrity verification mechanism that improves the effectiveness of digital signatures in detecting unauthorized modifications to the BIOS module while still allowing the image to undergo relocation.

Moreover, when BIOS is developed as a collection of digitally signed BIOS modules produced by different vendors, in certain situations, it may be

desirable to dynamically link these digitally signed modules. In particular, one BIOS module may be configured to make a call for a function coded in another BIOS module. However, in order to dynamically link the BIOS modules together, it would require modification of at least one BIOS module, which would  
5 invalidate any digital signature associated with the image of that BIOS module. Thus, the original digital signatures would not be effective to identifying unauthorized modification of the module. Thus, an integrity verification mechanism that overcomes this problem would be desirable.

#### 10 BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is an illustrative block diagram of a collection of software modules for loading as firmware into an electronic device.

15 Figure 2 is an illustrative block diagram of an embodiment of an electronic device utilizing the present invention.

Figure 3 is a block diagram of a first illustrative embodiment of the contents of the non-volatile memory component of Figure 2 that are collectively used to verify the integrity of relocated, post-relocation images using digital  
20 signatures.

Figure 4 is a block diagram of a second illustrative embodiment of the contents of the non-volatile memory component of Figure 2.

Figure 5 is a flowchart of the operations for verifying the integrity of stored information, such as a post-relocation image shown in Figures 3 and 4.

25 Figure 6 is a block diagram of a second illustrative embodiment of the present invention featuring a plurality of digitally signed images are dynamically linked together through one or more Bound & Relocated Import Tables (BRITs).

Figure 7 is a flowchart of the operations for generating a Bound and Relocated Import Table (BRIT).

30 Figure 8 is a flowchart of the operations for verifying the Bound and Relocated Import Table (BRIT) of Figure 7.

### DETAILED DESCRIPTION OF THE INVENTION

Herein, certain embodiments of the invention are described for verifying the integrity of information that is stored within an electronic device during pre-boot operations. In general, the stored information may include, for example, a  
5 digitally signed image that includes a post-relocation image of a software module or is dynamically linked with another digitally signed image.

In the following description, certain terminology is used to discuss features of the present invention. A “software module” comprises a set of instructions that  
10 perform a particular function. For example, the software module may feature instructions that are executed during a pre-boot cycle in order to initialize an electronic device. A replication of a binary representation of the instructions associated with the software module is referred to as an “image”. Different types of images can be used to represent different formatting stages. For instance, a  
15 “pre-relocation image” is a binary representation of the software module prior to conducting a relocation operation thereon. A “post-relocation image” is a binary representation of the module after relocation.

Furthermore, an “electronic device” is a combination of electronic hardware and software that collectively operates to perform one or more specific  
20 functions. Examples of an electronic device include a computer (e.g., a laptop, desktop, hand-held, server, mainframe, etc.), a component of the computer (e.g., a serial port), a cellular telephone, a set-top box (cable box, network computer, satellite television receiver, etc.), a network appliance and the like. A “link” is broadly defined as one or more information-carrying mediums to establish a  
25 communication pathway, including physical medium (e.g., electrical wire, optical fiber, cable, bus traces, etc.) or wireless medium (e.g., air in combination with wireless signaling technology).

Briefly, one integrity verification mechanism involves the configuration of a digitally signed image to include relocation information, a post-relocation image  
30 and a digital signature. The “relocation information” is a series of relative offsets from a base address. These offsets are generated after the stored information (e.g.,  
042390.P9144

an image of a software module) is compiled and placed into an executable format such as an MS-DOS® “EXE” format (MS-DOS is a registered trademark of Microsoft Corporation of Redmond, Washington). The offsets are converted to appropriate addresses during relocation when the base address, namely the storing address at which the image of the software module is stored and retrieved for execution, is determined. Thus, the post-relocation image differs from a pre-relocation image. The digital signature, however, is based on the pre-relocation image.

Another second integrity verification mechanism involves the inclusion of an import table and an export table within each digitally signed image. These tables allow functions within different digitally signed images to be dynamically bound together via a Bound & Relocated Import Table (BRIT). The BRIT resides outside the digitally signed image. Both of the integrity verification mechanisms may be performed by hardware or a software program embedded in a processor (described below) or simply executable by the processor.

Referring to Figure 1, an illustrative block diagram of a collection of “N” software modules ready for loading as firmware 100 into an electronic device is shown. Herein, each software module  $110_N$  ( $N \geq 1$ ) includes a header  $120_N$  and an image  $130_N$  for a particular software segment of the firmware 100. Prior to loading the software modules as firmware into a non-volatile memory as described below, each image  $130_N$  is digitally signed by a signatory to produce a digital signature  $140_N$ . The signatories may differ between each module or multiple modules may share the same signatory. A “signatory” may include any person or entity in a position of trust to guarantee or sponsor the digital signature (e.g., a bank, governmental entity, trade association, original equipment manufacturer, vendor, etc.).

Referring now to Figure 2, an illustrative block diagram of an embodiment of an electronic device is shown. For this embodiment, the electronic device 200 comprises a chipset 210 coupled to a processor 220 and a memory 230 through a first bus 240 and a second bus 250, respectively. In addition, chipset 210 is coupled to a third bus 260 that provides a pathway to one or more system



resources 270. Herein, the third bus 260 is represented as an input/output (I/O) bus (e.g., Peripheral Component Interconnect "PCI" bus); however, any other type of bus architecture may be used, including such bus architectures as Industry Standard Architecture (ISA), Extended ISA (EISA), Universal Serial Bus (USB) and the like. Herein, the third bus 260 is shown as a single bus, but it is contemplated that the third bus 260 may include multiple buses coupled together through bridge circuitry.

As shown, the system resources 270 would be coupled to at least one of the multiple buses. The system resources 270 comprise a communication device 280 and a non-volatile memory component 290. Communication device 280 is configured to establish communications with another electronic device over a communication link 285. Examples of communication device 280 include a network interface card, a modem card or an external modem. The non-volatile memory component 290 includes firmware that features digitally signed images of one or more software modules. In one embodiment, one or more of these software modules may form a Basic Input/Output System (BIOS) code of the electronic device 200. Examples of the non-volatile memory component 290 include a programmable, non-volatile memory such as flash memory, battery-backed random access memory (RAM), read only memory (ROM), erasable programmable ROM (EPROM), electrically erasable PROM (EEPROM), or any other type of memory appropriate for storing the module(s).

Referring to Figure 3, a block diagram of a first illustrative embodiment of the loading and storage contents of the non-volatile memory component 290 of Figure 2 is shown. The non-volatile memory component 290 is loaded with one or more digitally signed images 300, which collectively act as firmware. With respect to this embodiment, a digitally signed image 300 includes relocation information 310, a pre-relocation image 320 and a digital signature 330. The positioning of the elements forming any image is a design choice.

The relocation information 310 includes relative offsets 315 for certain routines within the pre-relocation image 310. Normally, the offsets 315 are generated when the software module associated with the digitally signed image is

compiled. The offsets 315 are used for properly addressing segments of information within the software module during relocation once the starting location of the image 300, referred to as base address "B\_ADDR," is determined. The relocation is conducted by a symmetrical relocation function that allows the relocated information to be undone for data integrity verification using the digital signature 330.

Herein, during relocation, the pre-relocation image 320 is converted (relocated) to a post-relocation image 340 is based on the pre-relocation image 320 of the image 300 during loading. Namely, the pre-relocation image 320 is relocated for retrieval from the base address (B\_ADDR) allotted to the image 300. In essence, the relocation operation adds B\_ADDR to the offsets 315 contained within the relocation information 310. This modifies the binary image such as the post-relocation image 340 stored in the non-volatile memory component now differs from the pre-relocation image 320 coded by the vendor.

The digital signature 330 includes at least a hash value of the pre-relocation image 320, which is digitally signed with a private key (PRK) of a signatory. Although the post-relocation image 340 now resides in the non-volatile memory component after relocation, it is appreciated that the digital signature 330 is based on the pre-relocated image 320 which is the binary form as originally produced before loading into the non-volatile memory component.

Referring to Figure 4, a block diagram of a second illustrative embodiment of the contents of the non-volatile memory component 290 is shown. The non-volatile memory component 290 contains multiple digitally signed images 410<sub>1</sub>-410<sub>M</sub> ("M" being a positive whole number) forming the firmware 400 (e.g., the BIOS). For instance, as an illustrative example, each digitally signed image 410<sub>1</sub>-410<sub>M</sub> is formed with a pre-relocation image 420<sub>1</sub>-420<sub>M</sub>, relocation information 430<sub>1</sub>-430<sub>M</sub> and a digital signature 440<sub>1</sub>-440<sub>M</sub>. Each digital signature 400<sub>1</sub>-400<sub>M</sub> is based on at least a hash value of its corresponding pre-relocation image 420<sub>1</sub>-420<sub>M</sub> and is digitally signed with a private key (PRK) of one or more signatories. Upon being loaded with the digitally signed images 410<sub>1</sub>-410<sub>M</sub>, the non-volatile memory component 290 undergoes a relocation operation which modifies the stored images

from the pre-relocation images 420<sub>1</sub>-420<sub>M</sub> to a post-relocation images 450<sub>1</sub>-450<sub>M</sub>, respectively.

Referring now to Figure 5, a flowchart of the operations for verifying the integrity of stored information, such as a post-relocation image of Figures 3 and 4, is shown. For integrity verification, the post-relocation image of a digitally signed image is reconverted to a pre-relocation image (block 500). This is accomplished using the relocation information contained in the digitally signed image. In particular, one or more arithmetic operations are performed on each offset; namely, as an example, the base address associated with memory of the non-volatile memory component is subtracted from each offset set forth in the relocation information. Thereafter, in block 510, a hash operation is performed on the reconverted, pre-relocation image to produce a hash value (referred to as the "reconverted hash value").

The digital signature of the digitally signed image is accessed and the hash value of the digital signature is recovered (block 520). This may be accomplished by running the digitally signed image through the digital signature algorithm being provided with a public key of the signatory for decode purposes. Thereafter, the recovered hash value is compared to the reconverted hash value (block 530). If a match is determined, the post-relocation image has been verified (block 540). Otherwise, the post-relocation image has not been verified, indicating that the image has been modified beyond such modification caused by relocation (block 550).

Figure 6 is a block diagram of a second illustrative embodiment of the present invention in which a plurality (M) of digitally signed images 600<sub>1</sub>-600<sub>M</sub> are dynamically linked together through one or more Bound & Relocated Import Tables (BRITs). Each BRIT corresponds to only one digitally signed image. It is contemplated that each digitally signed image 600<sub>1</sub>-600<sub>M</sub> may include a BRIT or only a subset of the digital signed images 600<sub>1</sub>-600<sub>M</sub> may be provided BRITs.

In this embodiment, a dynamic linking of two digitally signed images 600<sub>1</sub> and 600<sub>M</sub> is shown. Herein, the digitally signed image 600<sub>1</sub> includes a BRIT 610<sub>1</sub>, an import table 620<sub>1</sub>, an export table 630<sub>1</sub>, an image 640<sub>1</sub> based on selected

042390.P9144

information (e.g., a software module) and a digital signature 650<sub>1</sub>. The digital signature 650<sub>1</sub> is generated by conducting a one-way hash operation on the import table 620<sub>1</sub>, the export table 630<sub>1</sub> and the image 640<sub>1</sub> to produce a resultant hash value. The resultant hash value is digitally signed by a signatory using its private key.

In general, the import table 620<sub>1</sub> is listing of stored information located in another digitally signed image (e.g., image 640<sub>M</sub>) that need to be accessed for proper execution of the image 640<sub>1</sub>. The import table 620<sub>1</sub> comprises a plurality of entries 625 of which at least one entry (e.g., entry 626) of the import table 620 comprises an identifier 627 and a first offset 628. Generated either internally within the electronic device or remotely by a centralized authority, the identifier 627 indicates what segment(s) of information (e.g., a function, routine, code, data, etc.) not contained within the digitally signed image 600<sub>1</sub>, is required by the image 640<sub>1</sub> during execution. The identifier 627 may be represented as an alphanumeric name or a guaranteed unique identification (e.g., a sixteen-byte value). The first offset 628 is an offset pointer to an entry of the BRIT 610 that corresponds to entry 626.

The export table 630 is a listing of information contained in a digitally signed image that are available for other digitally signed images to retrieve.

Entries of the export table 630<sub>M</sub>, for example, include an identifier 635 for each segment of information included in the image 640<sub>M</sub> and a second offset 636. The second offset 636 is equivalent to an offset from an address location of the digitally signed image 600<sub>M</sub> to the address location of the segment of information required by image 640<sub>1</sub> of the digitally signed image 600<sub>1</sub>.

As shown, the BRIT 610<sub>1</sub> is associated with the digitally signed image 600<sub>1</sub>. Each entry of the BRIT 610<sub>1</sub> includes the identifier 627 and an address pointer 611 of the location of the segment of information. The address pointer 611 is an arithmetic combination of the starting address of the image 640<sub>M</sub> and the second offset 636. Thus, during execution of image 600<sub>1</sub>, a request for a segment of information referenced by the identifier 627 is routed via the BRIT 610<sub>1</sub> to a location within the image 640<sub>M</sub> as represented by dashed line 660. This enables

042390.P9144

the segment of information at that location to be accessed without modification of the image 640<sub>M</sub>. Thus, the digital signatures 650<sub>I</sub> and 650<sub>M</sub> can still be used to monitor modification of the import tables 620<sub>I</sub> and 620<sub>M</sub>, export tables 630<sub>I</sub> and 630<sub>M</sub>, and/or images 640<sub>I</sub> and 640<sub>M</sub>.

5 Referring now to Figure 7, a flowchart of the operations for generating a Bound and Relocated Import Table (BRIT) of the first digitally signed image 600, of Figure 6 is shown. Initially, all digitally signed images within the non-volatile memory component are located (block 700). Thereafter, an import table of the first digitally signed image is located (block 710). For an initial entry of the  
10 import table, the identifier is determined and a search is conducted for a matching identifier in an export table of another digitally signed images, namely any other digitally signed image besides the first digitally signed image (blocks 720 and 730).

15 If the matching identifier is not located, an error is reported (blocks 740 and 750). If the matching identifier is located within a second digitally signed image, for example, the offset in the export table that corresponds to the matching identifier and resides in second digitally signed image is arithmetically combined with the starting address of the second digitally signed image (blocks 740 and 760). The combined address is loaded into an entry of the BRIT along with the  
20 identifier associated with the import table (block 770). This process continues until all entries in the import table have corresponding entries in the BRIT (block 780).

Referring to Figure 8, a flowchart of the operations for verifying the Bound and Relocated Import Table (BRIT) of Figure 7 is shown. In this embodiment, a  
25 list of all digitally signed images is generated (block 800). For each digitally signed image, verify the integrity of these digitally signed images by confirming that its corresponding import table, export table and image have not been modified (block 810). For a first digitally signed image, for example, this can be accomplished by performing a hash operation on the import table, export table and  
30 image of the first digitally signed image. This produces a resultant hash value.

The resultant hash value is compared with a hash value uncovered from the digital

signature associated with the first digitally signed image. If the resultant hash value matches the recovered hash value, the import table, export table and image for the first digitally signed image have not been modified. This operation is continued for all of the remaining digitally signed images.

- 5           If the integrity of the digitally signed images cannot be verified, an error is reported (block 820). Otherwise, for the first digitally signed image, a determination is made whether the identifier in its import table matches an identifier in an export table of another digitally signed image (block 830). If no match is located, an error is reported (see block 820). If a match is located, a
- 10       determination is made whether the BRIT entry corresponding to the identifier of the import table points to an address defined by the matching identifier of the export table of another digitally signed image (block 840). Since the BRIT can only point to an address defined by an export table that is contained in a digitally signed image, it can only point to trusted information. If the BRIT entry
- 15       corresponding to the identifier of the import table points to an address defined by the matching identifier of the export table of another digitally signed image, the BRIT is verified (block 850). Otherwise, the BRIT is not verified (block 860).

- 20       While certain exemplary embodiments have been described and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not restrictive on the broad invention, and that this invention not be limited to the specific constructions and arrangements shown and described, since various other modifications may occur to those ordinarily skilled in the art.

CLAIMS

What is claimed is:

- 1           1.       Embodied in a memory component, a digitally signed image comprising:  
2           a post-relocation image being an image of a software module altered by a  
3           symmetrical relocation function upon loading of the image into the memory component;  
4           and  
5           a digital signature based on the image.
- 1           2.       The digitally signed image of claim 1, wherein the digital signature is a  
2           hash value of the image digitally signed by a private key of a selected signatory.
- 1           3.       The digitally signed image of claim 1 further comprising information for  
2           use by the symmetrical relocation function to convert the image into the relocation image.
- 1           4.       The digitally signed image of claim 3, wherein the information includes  
2           offsets for routines within the software module.
- 1           5.       The digitally signed image of claim 4, wherein the offsets are generated  
2           when the software module is compiled.
- 1           6.       Embodied in a memory component, a digitally signed image comprising:  
2           a Bound & Relocated Import Table (BRIT);  
3           an import table;  
4           an export table;  
5           an image of a software module; and  
6           a digital signature based on the import table, the export table and the image.

1           7.     The digitally signed image of claim 6, wherein the import table comprises  
2 a plurality of entries, each entry includes an identifier that indicates what segment of  
3 information contained in another digitally signed image is required by the image.

1           8.     The digitally signed image of claim 7, wherein the identifier includes a  
2 unique sequence of byte values.

1           9.     The digitally signed image of claim 7, wherein the identifier includes a  
2 unique sequence of alphanumeric characters.

1           10.    The digitally signed image of claim 7, wherein each entry of the import  
2 table further includes an offset to a corresponding entry of the BRIT.

1           11.    The digitally signed image of claim 6, wherein the export table includes a  
2 plurality of entries forming a listing of segments of information contained in the image, a  
3 selected entry of the plurality of entries includes an identifier of a segment of information  
4 associated with the segments of information.

1           12.    The digitally signed image of claim 11, wherein the selected entry further  
2 includes a second offset being an offset from a starting address of the digitally signed  
3 image to an address location of the segment of information.

1           13.    A method comprising:  
2           reconverting a post-relocation image of a digitally signed image back to a pre-  
3 relocation image, the pre-relocation image being an image of a software module prior to  
4 be altered by a symmetrical relocation function;  
5           conducting a hash operation on the reconverted, pre-relocation image to produce a  
6 reconverted hash value;



7 recovering a hash value from a digital signature contained in the digitally signed  
8 image, the hash value is based on the image of the software module; and  
9 comparing the hash value to the reconverted hash value.

1 14. The method of claim 13 further comprising: ~  
2 determining that an integrity of the post-relocation image remains intact if the  
3 hash value matches the reconverted hash value.

1 15. The method of claim 13 further comprising:  
2 determining that the post-relocation image has been modified beyond any  
3 modification caused by relocation when the hash value fails to match the reconverted  
4 hash value.

1 16. The method of claim 13, wherein the hash operation is a one-way hash  
2 operation.

1 17. A method for generating a Bound & Relocated Import Table (BRIT)  
2 within an electronic device, comprising:  
3 (a) locating an import table for a first digitally signed image loaded within the  
4 electronic device, each entry of the import table including an identifier and a first offset;  
5 (b) accessing an identifier within a selected entry of the first digitally signed image;  
6 (c) determining whether the identifier matches an identifier within an export table  
7 of a second digitally signed image loaded within the electronic device, the identifier for  
8 the export table is stored with a corresponding second offset; and  
9 (d) upon determining that the identifier within the selected entry matches the  
10 identifier within the export table,  
11 producing an address by combining the second offset with a starting  
12 address of the second digitally signed image, and  
13 loading the identifier within the selected entry and the address into an  
14 entry of the BRIT.

1 18. The method of claim 17 further comprising:  
2 repeating the operations of (a)-(d) for each remaining entry of the import table for  
3 loading resultant address and identifier pairs into different entries of the BRIT.

1 19. The method of claim 17, wherein the producing of the address by  
2 combining the second offset with the starting address of the second digitally signed image  
3 comprises an arithmetic operation.

1 20. The method of claim 17, wherein prior to locating an import table for the  
2 first digitally signed image, the method further comprises locating a plurality of digitally  
3 signed images loaded within the electronic device.

1 21. A method comprising:  
2 verifying an integrity of a plurality of digitally signed images loaded in an  
3 electronic device, the plurality of digitally signed images includes a first digitally signed  
4 image and a second digitally signed image;  
5 determining whether an identifier in an import table of the first digitally signed  
6 image matches an identifier in an export table of the second digitally signed image; and  
7 determining whether an entry of a Bound & Relocated Import Table (BRIT)  
8 corresponding to the identifier in the import table points to an address defined by the  
9 identifier in the export table.

1 22. The method of claim 21, wherein the verifying the integrity of the plurality  
2 of digitally signed images includes  
3 performing a hash operation on the import table, the export table and an image of  
4 the first digitally signed image to produce a first resultant hash value;  
5 recovering a first hash value from a digital signature contained in the first digitally  
6 signed image; and  
7 comparing the first hash value with the first resultant hash value.

1           23.     The method of claim 22, wherein the verifying the integrity of the plurality  
2 of digitally signed images further comprises  
3           performing a hash operation on an import table, an export table and an image of  
4 the second digitally signed image to produce a second resultant hash value;  
5           recovering a second hash value from a digital signature contained in the second  
6 digitally signed image; and  
7           comparing the second hash value with the second resultant hash value.

1           24.     An electronic device comprising:  
2           a processor; and  
3           a non-volatile memory component in communication with the processor, the non-  
4 volatile memory component includes including  
5           a post-relocation image being an image of a software module altered by a  
6 symmetrical relocation function upon loading of the image into the memory  
7 component, and  
8           a digital signature based on the image.

1           25.     The electronic device of claim 24, wherein the non-volatile memory  
2 component further includes information for use by the symmetrical relocation function to  
3 convert the image into the post-relocation image.

1           26.     The electronic device of claim 25, wherein the information placed within  
2 the non-volatile memory component includes offsets from a starting address of the image  
3 of the software module to a segment of information within the software module.

1           27.     An electronic device comprising:  
2           a processor; and  
3           a memory in communication with the processor, the memory being loaded with a  
4 Bound & Relocated Import Table (BRIT), an import table, an export table, an image of a

5 software module, and a digital signature based on the import table, the export table and  
6 the image.

1 28. The electronic device of claim 27, wherein the import table loaded within  
2 the memory comprises a plurality of entries, each entry includes an identifier that  
3 indicates what segment of information contained in another digitally signed image is  
4 required by the image.

1 29. The electronic device of claim 28, wherein the identifier associated with a  
2 particular entry includes a unique sequence of byte values.

1 30. The electronic device of claim 27, wherein the export table includes a  
2 plurality of entries forming a listing of segments of information contained in the image, a  
3 selected entry of the plurality of entries includes an identifier of a segment of information  
4 associated with the segments of information.

1 31. Embodied in a processor readable medium for execution by a processor, a  
2 software program comprising:

3 a first software module to reconvert a post-relocation image of a digitally signed  
4 image back to a pre-relocation image, the pre-relocation image being an image of a  
5 software module prior to be altered by a symmetrical relocation function;

6 a second software module to conduct a hash operation on the reconverted, pre-  
7 relocation image to produce a reconverted hash value;

8 a third software module to recover a hash value from a digital signature contained  
9 in the digitally signed image, the hash value is based on the image of the software  
10 module; and

11 a fourth software module to compare the hash value to the reconverted hash value.

1 32. The software program of claim 31 further comprising:

2 a fifth software module to determine that an integrity of the post-relocation image  
3 remains intact if the hash value matches the reconverted hash value.

1           33.   The software program of claim 31 further comprising a sixth software  
2 module to determine that the post-relocation image has been modified beyond any  
3 modifications caused by relocation when the hash value fails to match the reconverted  
4 hash value.

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100	2101	2102	2103	2104	2105	2106	2107	2108	2109	2110	2111	2112	2113	2114	2115	2116	2117	2118	2119	2120	2121	2122	2123	2124	2125	2126	2127	2128	2129	2130	2131	2132	2133	2134	2135	2136	2137	2138	2139	2140	2141	2142	2143	2144	2145	2146	2147	2148	2149	2150	2151	2152	2153	2154	2155	2156	2157	2158	2159	2160	2161	2162	2163	2164	2165	2166	2167	2168	2169	2170	2171	2172	2173	2174	2175	2176	2177	2178	2179	2180	2181	2182	2183	2184	2185	2186	2187	2188	2189	2190	2191	2192	2193	2194	2195	2196	2197	2198	2199	2200	2201	2202	2203	2204	2205	2206	2207	2208	2209	2210	2211	2212	2213	2214	2215	2216	2217	2218	2219	2220	2221	2222	2223	2224	2225	2226	2227	2228	2229	2230	2231	2232	2233	2234	2235	2236	2237	2238	2239	2240	2241	2242	2243	2244	2245	2246	2247	2248	2249	2250	2251	2252	2253	2254	2255	2256	2257	2258	2259	2260	2261	2262	2263	2264	2265	2266	2267	2268	2269	2270	2271	2272	2273	2274	2275	2276	2277	2278	2279	2280	2281	2282	2283	2284	2285	2286	2287	2288	2289	2290	2291	2292	2293	2294	2295	2296	2297	2298	2299	2300	2301	2302	2303	2304	2305	2306	2307	2308	2309	2310	2311	2312	2313	2314	2315	2316	2317	2318	2319	2320	2321	2322	2323	2324	2325	2326	2327	2328	2329	2330	2331	2332	2333	2334	2335	2336	2337	2338	2339	2340	2341	2342	2343	2344	2345	2346	2347	2348	2349	2350	2351	2352	2353	2354	2355	2356	2357	2358	2359	2360	2361	2362	2363	2364	2365	2366	2367	2368	2369	2370	2371	2372	2373	2374	2375	2376	2377	2378	2379	2380	2381	2382	2383	2384	2385	2386	2387	2388	2389	2390	2391	2392	2393	2394	2395	2396	2397	2398	2399	2400	2401	2402	2403	2404	2405	2406	2407	2408	2409	2410	2411	2412	2413	2414	2415	2416	2417	2418	2419	2420	2421	2422	2423	2424	2425	2426	2427	2428	2429	2430	2431	2432	2433	2434	2435	2436	2437	2438	2439	2440	2441	2442	2443	2444	2445	2446	2447	2448	2449	2450	2451	2452	2453	2454	2455	2456	2457	2458	2459	2460	2461	2
--	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	------	---

ABSTRACT

In one embodiment, a digitally signed image is embodied in a memory component such as a non-volatile memory. The digitally signed image comprises a post-relocation image and a digital signature. The post-relocation image is an image of a software module altered by a symmetrical relocation function by loading of the image into the memory component. The digital signature is based on the image so that it can be used to analyze data integrity.

09675413 002900

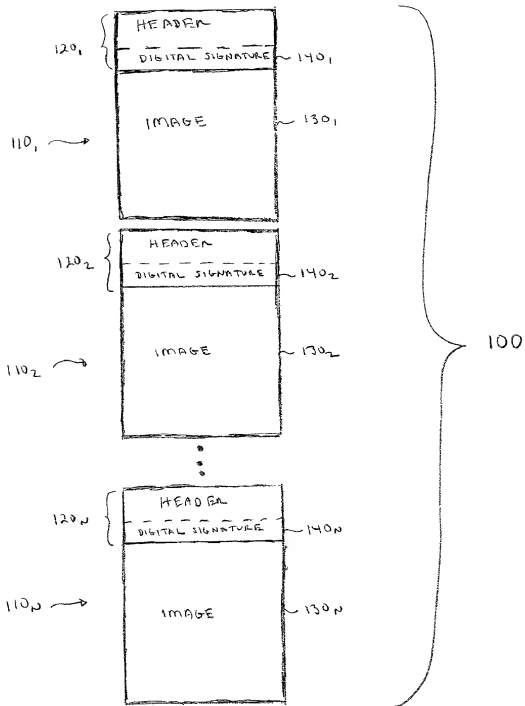
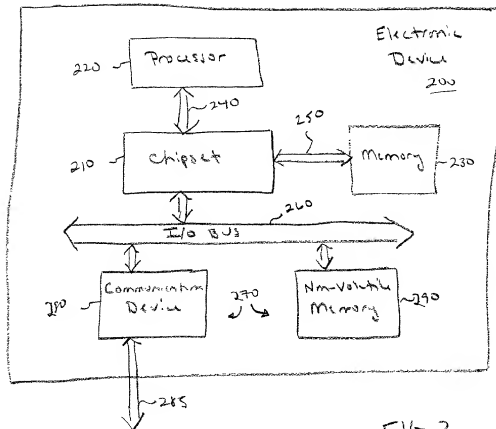


FIG. 1





00675113-002900

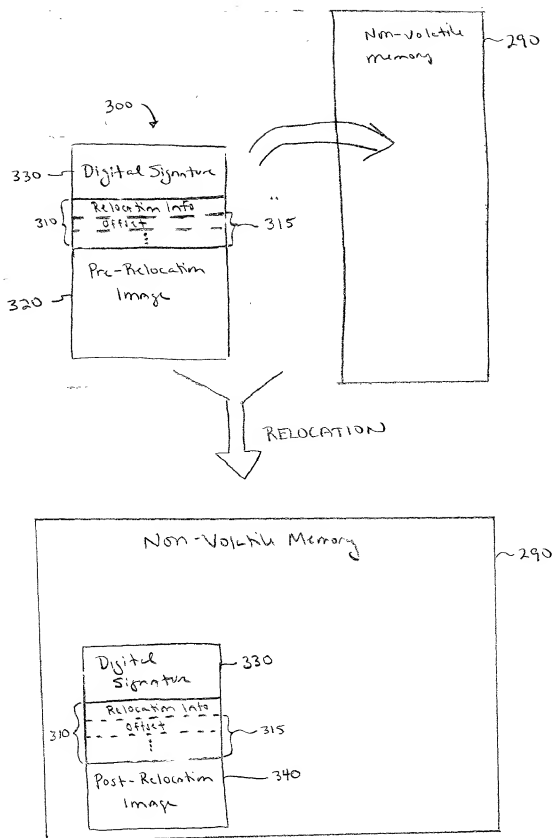


FIG. 3

0957413 002400

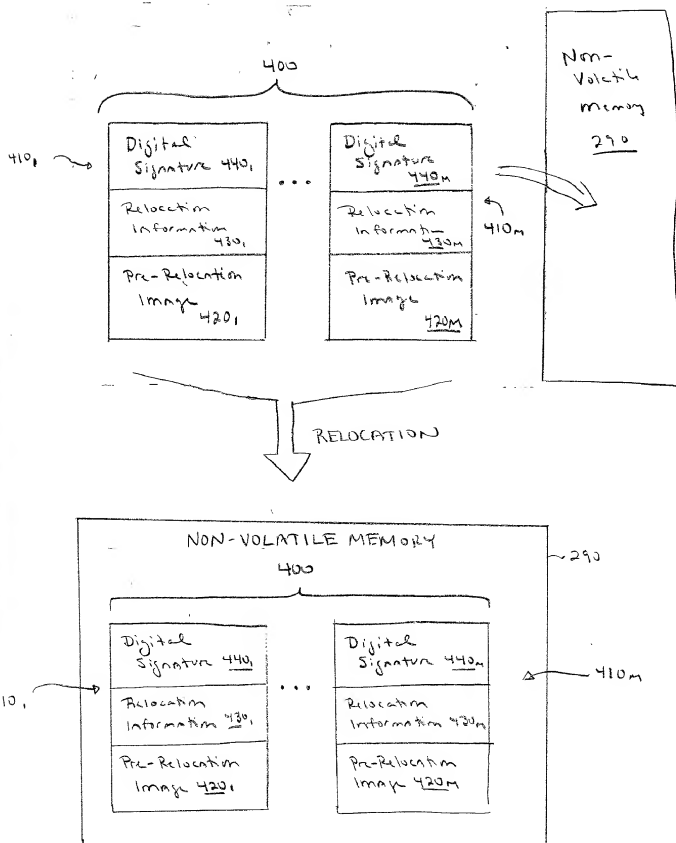


FIG. 4

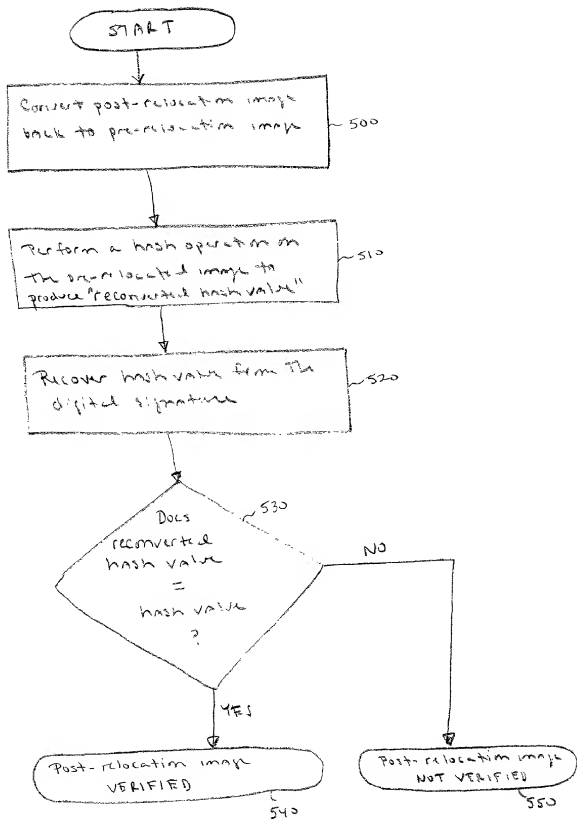
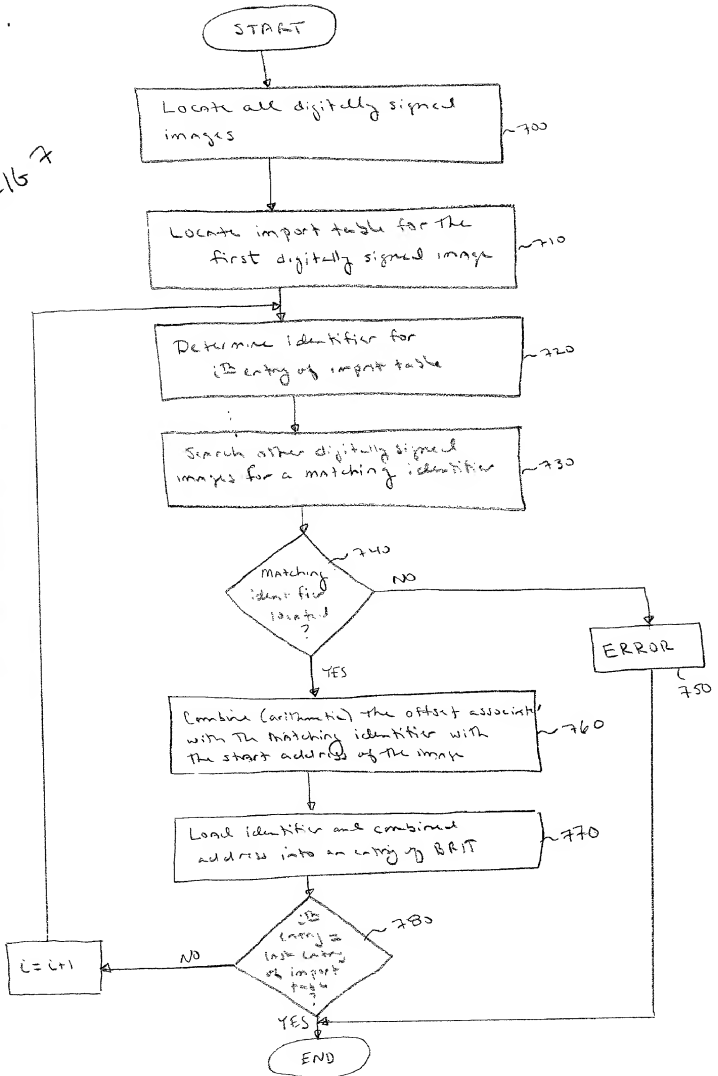


FIG. 5



FIG 7





# DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION (FOR INTEL CORPORATION PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

## A SYSTEM AND METHOD FOR VERIFYING THE INTEGRITY OF STORED INFORMATION WITHIN AN ELECTRONIC DEVICE

the specification of which

☒ is attached hereto.  
☐ was filed on \_\_\_\_\_ as \_\_\_\_\_  
 United States Application Number \_\_\_\_\_  
 or PCT International Application Number \_\_\_\_\_  
 and was amended on \_\_\_\_\_  
 (if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

APPLICATION NUMBER	COUNTRY (OR INDICATE IF PCT)	DATE OF FILING (day, month, year)	PRIORITY CLAIMED UNDER 37 USC 119
			<input type="checkbox"/> No <input type="checkbox"/> Yes
			<input type="checkbox"/> No <input type="checkbox"/> Yes
			<input type="checkbox"/> No <input type="checkbox"/> Yes

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

APPLICATION NUMBER	FILING DATE

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION NUMBER	FILING DATE	STATUS (ISSUED, PENDING, ABANDONED)

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to:

William W. Schaal, Reg. No. 39,018, BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

(Name of Attorney or Agent)

12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025 and direct telephone calls to:

William W. Schaal, (714) 557-3800.

(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**Full Name of Sole/First Inventor** (given name, family name)

**Robert P. Hale**

Inventor's Signature

Date

Residence Portland, Oregon USA

Citizenship USA

(City, State)

(Country)

P. O. Address 16451 NW Brandberry Drive

Portland, Oregon 97229 USA



**Full Name of Second/Joint Inventor** (given name, family name)

**Andrew J. Fish**

Inventor's Signature

Date

Residence Olympia, Washington USA

Citizenship USA

(City, State)

(Country)

P. O. Address 9630 Bee Dee Drive NE

Olympia, Washington 98516 USA

**Full Name of Third/Joint Inventor** (given name, family name)

Inventor's Signature

Date

Residence

Citizenship

(City, State)

(Country)

P. O. Address

**Full Name of Fourth/Joint Inventor** (given name, family name)

Inventor's Signature

Date

Residence

Citizenship

(City, State)

(Country)

P. O. Address

**Full Name of Fifth/Joint Inventor** (given name, family name)

Inventor's Signature

Date

Residence

Citizenship

(City, State)

(Country)

P. O. Address

## APPENDIX A

I hereby appoint BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, a firm including: William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. 42,261; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Lisa N. Benado, Reg. No. 39,995; Bradley J. Berezna, Reg. No. 33,474; Michael A. Bernadicon, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; R. Alan Burnett, Reg. No. 46,149; Gregory D. Caldwell, Reg. No. 39,926; Andrew C. Chen, Reg. No. 43,544; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Dennis M. deGuzman, Reg. No. 41,702; Stephen M. De Klerk, Reg. No. P46,503; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Sanjeet Dutta, Reg. No. P46,145; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; George Fountain, Reg. No. 36,374; Paramita Ghosh, Reg. No. 42,806; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W. Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Walter T. Kim, Reg. No. 42,731; Eric T. King, Reg. No. 44,188; Erica W. Kuo, Reg. No. 42,775; George B. Leavell, Reg. No. 45,436; Gordon R. Lindeen III, Reg. No. 33,192; Jan Carol Little, Reg. No. 41,181; Kurt P. Leyendecker, Reg. No. 42,799; Joseph Lutz, Reg. No. 43,765; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Clive D. Menezes, Reg. No. 45,493; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Daniel E. Ovanezian, Reg. No. 41,236; Kenneth B. Paley, Reg. No. 38,989; Marina Portnova, Reg. No. P45,750; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesti, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; Joseph A. Twarowski, Reg. No. 42,191; Thomas A. Van Zandt, Reg. No. 43,219; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Mark L. Watson, Reg. No. P46,322; Thomas C. Webster, Reg. No. P46,154; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Firasat Ali, Reg. No. 45,715; and Justin M. Dillon, Reg. No. 42,486; Raul Martinez, Reg. No. 46,904; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (714) 557-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg. No. 39,973; Sean Fitzgerald, Reg. No. 32,027; John N. Greaves, Reg. No. 40,362; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells, Reg. No. P43,256; Peter Lam, Reg. No. 44,855; Gene I. Su, Reg. No. 45,140; and Steven D. Yates, Reg. No. 42,242, my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.